Separability Criterion for One-Sided Gaussian Channels

Jason Hoelscher-Obermaier and Peter van Loock*

*Optical Quantum Information Theory Group, Max Planck Institute
for the Science of Light and Institute of Theoretical Physics I,
Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*

We show that the following nontrivial necessary precondition for an entanglement evolution equation for pure Gaussian states under one-sided Gaussian channels holds. Suppose a Gaussian quantum channel acts on one mode of a pure entangled multi-mode Gaussian input state. Then, for a fixed channel, either all output states are entangled or none of them are. In other words, if the input state is Gaussian, pure and entangled, the separability after a one-sided Gaussian quantum channel does not depend on the input state, but only on the channel. Furthermore, a simple linear-algebraic separability criterion allows to decide whether a given channel destroys the entanglement of pure entangled input states or leaves them entangled.

MOTIVATION

A large fraction of the known quantum information protocols (QIPs) — including such important protocols as quantum key distribution [1] and measurement-based quantum computation [2] — relies on entangled states. Unfortunately, entanglement is a quite fragile resource and unwanted interactions with the environment tend to destroy it rapidly. In order to assess the feasibility of many entanglement-based QIPs, it is therefore important to know how entanglement evolves in time.

A quantum system in state ρ which interacts with an environment in state ρ_E is in general subject to a non-unitary time evolution T

$$ T : \quad \rho \mapsto T(\rho) = \mathrm{tr}_E \left[U(\rho \otimes \rho_E) U^\dagger \right], \qquad (1) $$

where U is the time evolution of both the system and its environment. T is a completely positive, trace-preserving map from the set of density operators on a certain Hilbert space $\mathcal{H}$ into itself, a so-called *quantum channel*.

The standard way to calculate the evolution of entanglement under a given quantum channel is to directly calculate the evolution of the quantum state in question according to (1) and then calculate the entanglement of the output state $T(\rho)$. In particular, the calculation has to be performed separately for every input state. In the general case of arbitrary quantum channels and arbitrary (pure as well as mixed) input states, this is the only viable way.

Fortunately, we do not have to consider the most general quantum channel since typical noise effects can be described as *local quantum channels*, that is, they can be considered as acting uncorrelated on the different parts of the quantum system. It is therefore practically relevant to characterize the evolution of entanglement under local quantum channels [13]. As a special case of local quantum channels, this paper considers *one-sided quantum channels* which act only on a single qubit or a single mode of an entangled state.

QUBIT ENTANGLEMENT EVOLUTION EQUATION

In the qubit case, the restriction to one-sided quantum channels is known to simplify the calculation of the entanglement evolution drastically. More specifically, consider an arbitrary one-sided quantum channel $ which acts on one qubit of an initially pure two-qubit state $|\chi\rangle$ (hence the output state is $(\mathbb{1} \otimes \$)[|\chi\rangle \langle\chi|]$) and consider the evolution of the concurrence C under this channel [14]. Konrad et al. [3] have shown that, for all pure two-qubit input states $|\chi\rangle$, the concurrence of the output state is given by

$$ C \left\{ (\mathbb{1} \otimes \$)[|\chi\rangle \langle\chi|] \right\} = C \left\{ (\mathbb{1} \otimes \$)[|\Phi\rangle \langle\Phi|] \right\} \cdot C \left\{ |\chi\rangle \langle\chi| \right\}, \tag{2} $$

where $|\Phi\rangle$ is one of the Bell states. Hence, up to a prefactor given by the entanglement of the input state, the entanglement (as quantified by the concurrence) evolves always exactly like the entanglement of the Bell states.

In particular, this implies that a given one-sided quantum channel will either disentangle all initially entangled pure two-qubit states or leave all of them entangled. For if the initial state $|\chi\rangle$ is entangled, we have $C \left\{ |\chi\rangle \langle\chi| \right\} \neq 0$ and therefore, according to (2), the entanglement of the output state is zero if and only if $C \left\{ (\mathbb{1} \otimes \$)[|\Phi\rangle \langle\Phi|] \right\} = 0$ — independent of the state $|\chi\rangle$.

GAUSSIAN ENTANGLEMENT EVOLUTION

Equation (2) is relevant because qubits are ubiquitous in quantum information. But in many quantum-optical implementations of QIPs, continuous variables are preferred over qubits because of practical advantages [15]. In continuous variable quantum information processing, Gaussian states are widely used and typical errors are described by Gaussian quantum channels. Therefore, an evolution equation for the entanglement of Gaussian states under one-sided Gaussian channels similar to (2) would be highly relevant. But, an equation of the

form (2) in the Gaussian regime would require that — just as in the qubit case — the separability after the one-sided Gaussian channel depends only on the channel and not on the input state. Before this fact is proved, some basic concepts of the theory of Gaussian states have to be introduced.

Gaussian Channels and Covariance Matrices

Consider a mode of the electro-magnetic field with annihilation and creation operators $\hat{a}, \hat{a}^\dagger$. The *quadratures* $\hat{q}, \hat{p}$ are defined by

$$\hat{q} = \frac{1}{\sqrt{2}} \left(\hat{a} + \hat{a}^\dagger \right), \quad \hat{p} = \frac{1}{\sqrt{2}\,\mathrm{i}} \left(\hat{a} - \hat{a}^\dagger \right). \qquad (3)$$

Every quantum state of the field corresponds uniquely to a Wigner function which can be considered as a quasi-probability distribution over the possible measurement results for the quadratures. *Gaussian states* are states whose Wigner function is a Gaussian distribution. In particular, they are completely characterized by the expectation values and variances of the quadrature operators. The expectation values can be set to zero by local operations and are therefore irrelevant for the entanglement of the state. All the interesting information is contained in the variances which are conveniently summarized in the *covariance matrix* (CM). The CM of a two-mode state ρ_{AB} on modes A and B is a real symmetric 4×4 matrix σ_{AB} with entries

$$(\sigma_{AB})_{ij} = \frac{1}{2} \langle \hat{R}_i \hat{R}_j + \hat{R}_j \hat{R}_i \rangle - \langle \hat{R}_i \rangle \langle \hat{R}_j \rangle, \qquad (4)$$

where $\hat{R} = (\hat{q}_A, \hat{p}_A, \hat{q}_B, \hat{p}_B)$ is the vector containing the quadratures and $\langle \hat{X} \rangle$ is the expectation value of the operator $\hat{X}$ in the state ρ_{AB}. Note that not every real symmetric 4×4 matrix is the CM of a quantum state since the variances have to fulfill the Robertson-Schrödinger inequality. If we write σ_{AB} in block form

$$\sigma_{AB} = \begin{pmatrix} \alpha & \gamma \\ \gamma^{\mathrm{T}} & \beta \end{pmatrix} \qquad (5)$$

(with real 2×2 matrices α, β, γ), the Robertson-Schrödinger inequality is fulfilled exactly if (see [5])

$$\det[\alpha] + \det[\beta] + 2\det[\gamma] \leq 4\det[\sigma_{AB}] + 1/4. \qquad (6)$$

For future reference we also note that the separability of σ_{AB} is equivalent to

$$\det[\alpha] + \det[\beta] - 2\det[\gamma] \leq 4\det[\sigma_{AB}] + 1/4. \qquad (7)$$

The most important example of an entangled two-mode Gaussian state is the two-mode squeezed state with CM

($\mathbb{1}_n$ denotes the $n \times n$ identity matrix)

$$\gamma_{\mathrm{TMSS,r}} = \frac{1}{2} \begin{pmatrix} \cosh(r)\mathbb{1}_2 & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{1}_2 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ r > 0. \qquad (8)$$

A *Gaussian quantum channel* is defined as a quantum channel which maps Gaussian states onto Gaussian states. To calculate the evolution of the entanglement, we only need to consider the action of the channel on the CM. For future convenience, let us define the abbreviation $A[B] \equiv ABA^{\mathrm{T}}$ if A and B are matrices. If a Gaussian channel $\mathcal{G}$ acts only on mode B of a two-mode Gaussian state, the initial CM σ_{AB} evolves as (see [6])

$$\sigma_{AB} \xrightarrow{\mathbb{1} \otimes \mathcal{G}} (\mathbb{1} \oplus f)[\sigma_{AB}] + (\mathbb{0} \oplus g), \qquad (9)$$

where f and g are two real 2×2 matrices which completely characterize the channel $\mathcal{G}$, $\mathbb{0}$ represents the zero matrix, and $\oplus$ denotes the matrix direct sum. Since the g-contribution is independent of the state σ_{AB}, it can be thought of as a noise term. Note that not every pair of matrices f, g describes a Gaussian quantum channel since the output state must again respect the Robertson-Schrödinger inequality as embodied by (6). Channel matrices f, g which describe a genuine Gaussian channel fulfill (see [6])

$$4\det[g] \geq (\det[f] - 1)^2. \qquad (10)$$

Separability Criterion for Gaussian Channels

Proposition 1: *If a one-sided Gaussian quantum channel $\mathcal{G}$, which is characterized by channel matrices f and g, acts on mode B of a pure and entangled two-mode Gaussian state with covariance matrix σ_{AB}, then the output state $(\mathbb{1} \oplus f)[\sigma_{AB}] + (\mathbb{0} \oplus g)$ is separable if and only if*

$$4\det[g] \geq (\det[f] + 1)^2. \qquad (11)$$

The same condition (11) is also equivalent to the separability of the output state if the channel acts on a single mode of a Gaussian state on more than two modes.

This means that, for initially pure and entangled states, the separability of the output state depends only on the properties of the channel and not on the properties of the initial state. Accordingly, every one-sided Gaussian channel can easily be classified as "disentangling" or "non-disentangling" via the separability condition (11). Note that this is quite counterintuitive: For any two Gaussian states X and Y — no matter how slightly entangled X and how strongly entangled Y — there is no one-sided Gaussian channel that destroys the

entanglement of X and leaves some of the entanglement of Y intact [16].

Holevo [8] provided general conditions under which Gaussian channels disentangle all input states, which are in agreement with (11). His results, however, do not imply that any Gaussian channel which leaves some pure entangled Gaussian input state entangled must leave all such states entangled, as required for the existence of a Gaussian entanglement evolution equation.

Note also the close similarity of the separability condition (11) and the physicality condition (10) for the channel matrices. For any two real matrices f, g, there is a quantum channel such that f, g describe its action on CMs according to (9) if the determinant of the noise matrix g is large enough, i.e. if $4 \det[g] \geq (\det[f] - 1)^2$. If g also fulfills $4 \det[g] \geq (\det[f] + 1)^2$, this channel will only output separable states.

Proof of Proposition 1. Every pure, entangled two-mode Gaussian state σ_{AB} is related to a two-mode squeezed state $\gamma_{\mathrm{TMSS,r}}$ via local unitary operations which act on the CM as symplectic matrices S_A and S_B [9]

$$\sigma_{AB} = (S_A \oplus S_B)[\gamma_{\mathrm{TMSS,r}}], \qquad (12)$$

where again the abbreviation $A[B] \equiv ABA^{\mathrm{T}}$ has been used. The transformation S_A of mode A commutes with the channel which acts on mode B and can be undone after the channel since local unitary operations do not change the entanglement of the output state. Therefore, using (12), the separability of the output state $(\mathbb{1} \oplus f)[\sigma_{AB}] + (\mathbb{0} \oplus g)$ is equivalent to the separability of the state

$$(\mathbb{1} \oplus fS_B)[\gamma_{\mathrm{TMSS,r}}] + (\mathbb{0} \oplus g) = \begin{pmatrix} C & S(fS_B)^T \\ fS_B S & fS_B[C] + g \end{pmatrix}$$
$$\equiv \begin{pmatrix} \alpha & \gamma \\ \gamma^{\mathrm{T}} & \beta \end{pmatrix}, \qquad (13)$$

where $C \equiv 1/2 \cosh(r) \mathbb{1}_2$ and $S \equiv 1/2 \sinh(r) \sigma_z$. According to (7), the separability of (13) is equivalent to

$$\det[C] + \det[fS_B[C] + g] - 2\det[fS_B S]$$
$$\leq 4\det[(\mathbb{1} \oplus fS_B)[\gamma_{\mathrm{TMSS,r}}] + (\mathbb{0} \oplus g)] + 1/4. \quad (14)$$

Now there are two cases. Assume first that $\det[f] = 0$. In this case, the channel separability condition (11) is automatically fulfilled because any Gaussian channel also fulfills (10). Therefore, it has to be shown that, in this case, the output state is indeed separable, as implied by (11) together with (10).

For $\det[f] = 0$, we have $\det[\gamma] = \det[fS_B S] = \det[f]\det[S_B S] = 0$ and the separability condition (7) reduces to

$$\det[\alpha] + \det[\beta] - 2\det[\gamma] \overset{\det[\gamma]=0}{=} \det[\alpha] + \det[\beta]$$
$$\leq 4\det[\sigma] + 1/4 \qquad (15)$$

But, under the same conditions (for $\det[f] = 0$), the separability condition (15) is implied by condition (6) which expresses the physicality of the output CM:

$$\det[\alpha] + \det[\beta] + 2\det[\gamma] \overset{\det[\gamma]=0}{=} \det[\alpha] + \det[\beta]$$
$$\leq 4\det[\sigma] + 1/4. \qquad (16)$$

Therefore, if $\det[f] = 0$, the output state is indeed separable.

Assume now that $\det[f] \neq 0$, hence f is invertible. Using that $\det[S_B] = 1$ for every symplectic matrix S_B, equation (14) can be rewritten as

$$\det[C] + \det[f]^2 \det[C + S_B^{-1}f^{-1}[g]] - 2\det[f]\det[S]$$
$$\leq 4\det[f]^2 \det[\gamma_{\mathrm{TMSS,r}} + (\mathbb{0} \oplus S_B^{-1}f^{-1}[g])] + 1/4. \qquad (17)$$

Using that $S_B^{-1}f^{-1}[g]$ is a symmetric matrix, this inequality can be evaluated (using computer algebra) and reduces to

$$4\det[g] \geq \det[f]^2 + 2\det[f] + 1 = (\det[f] + 1)^2, \quad (18)$$

which establishes (11).

The generalization to the case of a Gaussian channel acting on one mode of a pure N-mode Gaussian state is straightforward: Any pure N-mode Gaussian input state can be transformed via a local $(N-1)$-mode unitary $S_{A,N-1}$ and a local one-mode unitary S_B into a two-mode squeezed state on the mode A_{N-1} and the mode B as well as $N-2$ unrelated modes $(A_1, \ldots, A_{N-2})$ in the vacuum state with CM $\gamma_{\mathrm{vac}} = \frac{1}{2}\mathbb{1}$ [7]:

$$\sigma_{A_1,\ldots,A_{N-1},B} = \qquad\qquad (19)$$
$$(S_{A,N-1} \oplus S_B)\left[(\gamma_{\mathrm{vac}})_{A_1,\ldots,A_{N-2}} \oplus (\gamma_{\mathrm{TMSS,r}})_{A_{N-1},B}\right].$$

Again, the unitary $S_{A,N-1}$ can be interchanged with the channel (which only acts on mode B) and undone. From here on, the proof for the case of an N-mode input state works exactly like the two-mode case since the modes in the vacuum state are irrelevant for the entanglement of the two modes in the two-mode squeezed state. $\qquad\square$

Summing up, *qualitatively*, the entanglement of all pure Gaussian states evolves in the same way under a fixed one-sided Gaussian channel: Just as in the qubit case, the separability of the output state depends only on the channel, not on the initial state. The question whether or not it also evolves in the same way *quantitatively*, hence whether or not a full Gaussian entanglement evolution equation similar to (2) exists, is still open. The answer to this question depends crucially on the choice of the right entanglement measure for a Gaussian version of (2). Numerical calculations ruled out the existence of a Gaussian entanglement evolution equation for the two best-known entanglement measures in the context of

Gaussian quantum information theory, the entanglement of formation and the logarithmic negativity [10] — but, of course, this does not imply that no such equation can exist.

Addendum: Right after completion of this work, Wang et al. [11] indeed published a Gaussian entanglement evolution equation using a different entanglement measure which is introduced in their article. This entanglement measure is a non-standard entanglement of formation based upon the shortest distance measure for pure states. Against the background of our numerical nogo results for a potential, quantitative entanglement evolution equation using the standard entanglement of formation [10], the results of ref. [11] based on a non-standard entanglement of formation are very surprising.

---

* Electronic address: peter.vanloock@mpl.mpg.de

[1] M. Curty, M. Lewenstein, und N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[2] R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[3] T. Konrad, F. de Melo, M. Tiersch, C. Kasztelan, A. Aragao, and A. Buchleitner, Nature Physics **4**, 99-102 (2008).

[4] S.L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[5] A. Ferraro, S. Olivares, and M.G.A. Paris, Bibliopolis, Napoli (2005), ISBN 88-7088-483-X; quant-ph/0503237 (2005).

[6] J. Eisert and M.M. Wolf, in *Quantum Information with Continuous Variables of Atoms and Light*, N.J. Cerf, G. Leuchs, and E.S. Polzik, Eds., pages 23-42 (Imperial College Press, London, 2007); quant-ph/0505151 (2005).

[7] A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2003).

[8] A.S. Holevo, Problems of Information Transmission **44** (3), 171-184 (2008); quant-ph/0802.0235 (2008).

[9] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).

[10] J. Hoelscher-Obermaier, Diplom thesis, University of Regensburg (2009).

[11] X. Wang, Z. Yu, and J. Hu, quant-ph/1001.0156 v3 (2010).

[12] W.K. Wootters, Phys. Rev. Lett. **80**, 2245-2248 (1998).

[13] Local quantum channels also play a very important role in quantum communication because they include the lossy and noisy fiber channels which come up in the context of entanglement distribution.

[14] The use of the concurrence is essential because the proof of (2) relies on the analytic formula for the concurrence of arbitrary (pure and mixed) two-qubit states [12].

[15] For example, continuous variable implementations are usually deterministic while qubit protocols are often probabilistic. See, for example, [4] for a recent review of continuous variable quantum information processing.

[16] This is particularly counterintuitive since the entanglement of Gaussian states is unbounded. Hence, the entanglement of the state Y can be arbitrarily high.